13th ICCRTS
"C2 for Complex Endeavors"

Disruptive Effects of Net-Centricity on Command and Control

Primary TOPIC 5: Organization Issues
Secondary TOPIC 1: C2 Concepts, Theory, and Policy
Tertiary TOPIC 4: Cognitive and Social Issues

Dr. John S. Bay
Air Force Research Laboratory, Information Directorate
26 Electronic Parkway
Rome, New York 13341

(315) 330-4512
john.bay@rl.af.mil

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE **JUN 2008**	2. REPORT TYPE	3. DATES COVERED **00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE **Disruptive Effects of Net-Centricity on Command and Control**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Laboratory,Information Directorate,26 Electronic Parkway,Rome,NY,13341**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S) 11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

13th International Command and Control Research and Technology Symposia (ICCRTS 2008), 17-19 Jun 2008, Seattle, WA

14. ABSTRACT

This paper explores the potential for net-centric operating environments to disrupt traditional practices in command and control. We conclude that at least two major disruptive effects are likely: information non-attribution and control decentralization. Information non-attribution reverses the assumption that commands are issued from an individual entity to an individual entity. In net-centric worlds, orders will be issued to a resource pool, and information will be gleaned from an infosphere. The military command hierarchy must therefore get accustomed to issuing orders to ?nobody in particular,? and commanders will lack an individual subordinate with whom to attribute the responsibility. Conversely, they must accept information from the infosphere without the trust inherited from known reliable providers. Control decentralization is a tendency for decision-making to migrate to the ?edges? of the organization, where the most direct sensors and effectors are physically located. Net-centricity directly empowers those closest to the action by giving them access to information of quality and quantity that is potentially equal to or better than that available in command centers. Together, these effects of net-centricity suggest disruptive changes in command and control practices that must be modeled and explored as the vision of net-centric command and control becomes a reality.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**30**	

13th ICCRTS
"C2 for Complex Endeavors"

Disruptive Effects of Net-Centricity on Command and Control

Dr. John S. Bay
Air Force Research Laboratory, Information Directorate
26 Electronic Parkway
Rome, New York 13341

(315) 330-4512
john.bay@rl.af.mil

Abstract

This paper explores the potential for net-centric operating environments to disrupt traditional practices in command and control. We conclude that at least two major disruptive effects are likely: *information non-attribution* and *control decentralization*.

Information non-attribution reverses the assumption that commands are issued *from* an individual entity *to* an individual entity. In net-centric worlds, orders will be issued to a *resource pool*, and information will be gleaned from an *infosphere*. The military command hierarchy must therefore get accustomed to issuing orders to "nobody in particular," and commanders will lack an individual subordinate with whom to attribute the responsibility. Conversely, they must accept information from the infosphere without the trust inherited from known reliable providers.

Control decentralization is a tendency for decision-making to migrate to the "edges" of the organization, where the most direct sensors and effectors are physically located. Net-centricity directly empowers those closest to the action by giving them access to information of quality and quantity that is potentially equal to or better than that available in command centers.

Together, these effects of net-centricity suggest disruptive changes in command and control practices that must be modeled and explored as the vision of net-centric command and control becomes a reality.

Introduction: Disruptive Innovation

Before defining and describing net-centricity as the forcing function of new military behaviors, it is useful to understand why it deserves a critical look. In [5], the term *disruptive technology* is used to describe a technology that gains a market foothold despite inferior performance by virtue of its appeal to the wider market of low-end users. Those users value different dimensions of the product, and are therefore largely ignored by big-market forces that value sustaining innovations on existing trajectories.

Thus, technologies that exceed customer expectations too quickly are vulnerable to disruptive technologies. When the disruptive innovation gains market share, and old customers adopt new products, the net performance of products in the users' hands actually drops. However, it is observed that customer expectations of performance do grow over time, so the new technology is driven to rapid innovation so that it will retain its market share and not succumb to further disruptors. So it is important to remember that disruptive technologies are not merely those that have introduced steep performance improvements, but which, at the time of their introduction, were inferior in some way to the incumbent. As Figure 1 illustrates, the net performance of the technology in the users' hands actually has a negative discontinuity at this point of disruption. This is counter to the popular misconception that "disruptive" implies a positive discontinuity. While such profiles exist, they are less interesting because there is no difficult decision-point for the consumer; all other things being *equal*, one should always adopt the better technology.

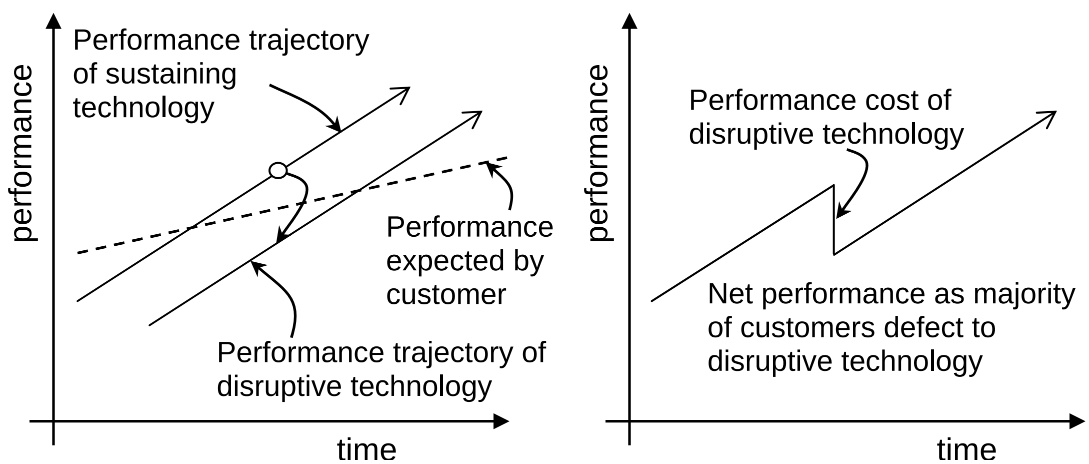


Figure 1. Disruptive innovations are introduced at lower levels of performance, but gain market share because of shifting values of the consumers/users. Thus, the market at some point adopts lower-performing technologies. Disruptive technologies are thereby distinguished from discontinuous sustaining innovations.

Net-centric information environments are proving themselves to be disruptive innovations. The eventual superiority of them is widely recognized [1, 7, 16], or perhaps simply assumed. They have the potential to facilitate the fusion and delivery of arbitrary sets of information to consumers around the globe in ways that point-to-point connection-oriented information transfer mechanisms cannot. The rapid adoption of service-oriented and information-centric architectures will clearly lead to superior performance attributes.

But what about the initial disruption? Is it true that the introduction of net-centric information environments will occur with a performance sacrifice relative to connection-oriented environments? Certainly this is true if one considers legacy transmission and storage technologies; there is a very real cost of adoption in the infrastructure alone.

The purpose of this paper is to consider more functional forms of disruption. If we assume away the costs of the infrastructure of net-centricity, what are the costs associated with the way we use and think about the technology? What do we sacrifice in favor of the promise of Metcalfe's Law, which states that the utility of a network scales as the square of the number of nodes it connects [1]?

Rosenberg [15] has documented the informal observation among military leaders that command and control doctrine is being challenged by network-centric operations. In particular, he discusses the challenges of commanding a young force that is technologically savvy and has access to the same (or better) information sources available as the commander. He ponders the willingness of future troops to follow a commander's orders to engage in perilous mission – one wherein the losses may be expected to be high – if in fact the warfighters knew exactly what awaits them. This potential for information-empowered behavior is predicted in both directions. From the top-down, the potential for micro-management is envisioned as a result of our commanders' ability to instantly acquire knowledge from the field. From the bottom up, senior leaders are quoted describing ways in which decision-making has migrated to the tactical edges, leading to a flattening of the command and control hierarchy. As a result, the role of commander's intent has begun to dominate the role of commander's explicit direction.

In this paper, we will show the technological reasons and historical precedent for the bottom-up phenomenon; i.e., that network-centric environments will lead to decentralization of command and control. In the conclusion, we will assert that this will further motivate innovation in the long-established and largely successful doctrine of the U.S. military.

Net-Centricity Characterized

In [7], net-centric environments are defined as

> *… a framework for full human and technical connectivity and interoperability that allows all DoD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence; and protects information from those who should not have it*

The Network Centric Operations Industry Consortium [12] defines the term net-centric to mean:

> *Related to systems and patterns of behavior that are influenced significantly or enabled by current and emergent networks and network*

> *technologies. Often these center around IP-based internetworking, but the term is sometimes used to include any type of enabling network.*

Note that both of these definitions focus on the utility of net-centricity; that is, the activities that are afforded the user, rather than simply the structure of the environment or network. Thus it is critical to consider utility in an examination of net-centricity as a disruptive technology.

Some other observations about net-centricity are important. First, note that strictly, the term is an oxymoron in that net-centric environments inherently have no *center*. It is their decentralization that is their most important defining characteristic, from which many of net-centricity's benefits derive.

Also, lest the term lose its meaning through over-use and misuse, it is worth identifying attributes that, taken by themselves, do ***not*** constitute net-centricity:

- **Wireless devices –** Simply endowing a device with a communications capability does not make it part of a net.
- **Web-enabled –** Likewise, web-enabling an information service or device makes it http compliant, but does not mean it contributes to the functionality described in the above definitions.
- **Interoperability –** Interoperability can be achieved with standardized interfaces and does not alone imply super-linear functionality.
- **Systems based on a closed network infrastructure –** This would make them static and non-adaptive; such as a distributed appliance.
- **High-bandwidth –** Though it can be argued that broadband communications are necessary for net-centricity, it is not sufficient.

Instead, it is more to our point to extrapolate on the terms in the above definitions to further characterize net-centric environments and the information they contain. As discussed in [16], the information in a net-centric system is:

- **Visible –** It exists in a shared space and contains meta-data that can be discovered and cataloged.
- **Accessible –** Mechanisms are provided to request and retrieve information.
- **Understandable –** Communities of interest can be formed so that special information formats or presentations can be created and tailored to these classes of users.
- **Trusted –** Some pedigree or security metadata is also attached, or there exists a lineage to a trusted source.
- **Interoperable –** An open information standard is rigorously defined and published, so that new information and sources can be added at any time.
- **Responsive –** An information store with no mechanism to adapt to new use models or information contents will soon become obsolete.

While these attributes are characteristic to all net-centric information environments, there are some subtleties in the practical ways in which systems are implemented that will be important for our discussion.

First, if the system is truly large scale, such as the DoD-wide Global Information Grid (GIG), then although it is desirable for all information to have a pedigree, it is unreasonable to consciously and deliberatively track it for every piece of information received. To be truly convenient, information would come in a fused form that combines facts, features, or other information components. That is, information is returned from the "pool" of resources (or *infosphere*) in such a way that trace-back of individual components is impractical and unimportant to the user. In many cases, a search or query for information will return a variety of components, with a corresponding variety of pedigrees. For example, if a user asks for an overhead view of a certain city, and an overhead map is returned, how often would that user then delve into the provenance of that map before making use of it, particularly if the information came from a government channel and therefore carried an implied measure of information assurance? If the map was created by mosaicking a number of patches, it is unimportant to the user that those patches may have come from different sources. The value of the information is simply taken for granted once it passes an initial cursory verification (for example, when a user recognizes Central Park and the outline shape of Manhattan Island, then he will most likely accept the other details of the map as true.)

Second, and conversely, when a query is made, it is not made to an individual provider. In the above example, it would make no sense for a user to make a request for a map of New York City and, fully aware that he has a pooled information resource at his disposal, ask that it be delivered by one individual provider. Certainly there are diagnostic reasons that one might want to query a specific provider, but if we want information, we search as broadly as possible.

Thus, in a net-centric environment, a user must become comfortable accepting information "from nobody in particular," and issuing requests "to nobody in particular." but yet, we must accept this mode of operation in order for net-centricity to be useful. However, it is anathema to conventional command and control doctrine. This is the behavior that will present challenges to military users. Taking this service model to its logical next step would give us the "cloud computing" paradigm. In cloud computing, a user needing computational services and horsepower beyond his local resources uses the Internet to transparently access other computing services and data warehouses in a seamlessly coherent way. Although the technological problems associated with distributed execution and synchronization of the computations are formidable, in an ideal case the end user would not have to trouble himself with "who" is doing his computing.

The graphic illustration of this concept that the U.S. Department of Defense uses is the "plasma lamp," as shown in Figure 2. The important feature of this illustrative device is that when a user touches the globe to get information, it is the entire *body* of information that is being accessed. Consumers never directly connect with suppliers.

A concrete example of the difference between a *networked* system and a *network-centric* system is the *unattended sensor network*. If we perform the thought-experiment of providing a warfighter with sensors one at a time, we will see the transition between the concepts. Suppose we were to give a dismounted soldier a sensor with which he can better perceive the enemy. In most cases, we would all see this as a benefit. If we give him two sensors, it is still probably to his benefit. If we continue this process, we quickly reach a point at which our hypothetical soldier will say, "stop! I will do without!" Now suppose we propose a network of 1000 sensors, and tell the soldier that he does not have to operate or even read each sensor; the fused, fully-interpreted information that the network detects will be provided to him in a single piece. That would be a network-centric system, and also a disruptive technology (which "disrupted" at the point at which he was overwhelmed with distinct sensors).

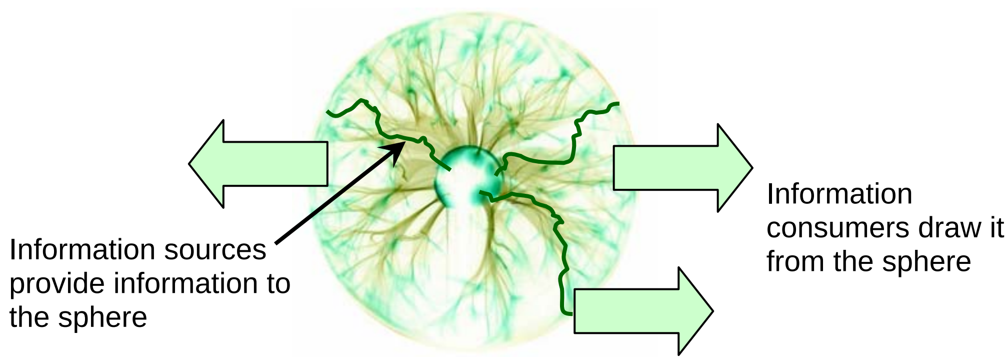


Figure 2. The U.S. Department of Defense uses the "plasma lamp" image to describe net-centricity (http://www.defenselink.mil/cio-nii/other/video.shtml). The analogy is that all information flows into the sphere, which surrounds us and thus makes the information available to all. It is the topological counterpoint to connection-oriented networking.

Observations from Popular Culture

The power of net-centricity can be readily observed in non-defense applications. One can look at blogs, Google, Napster, or Wikipedia to see the power of collaborative information sharing. These information sources have become second-nature information stores in modern culture, and one can even observe television news programs basing their reporting on data found in a blog or on YouTube. The parallel to Wikipedia was observed in [15]. Wikipedia now has over 2,000,000 English language articles, and over 10,000,000 total pages [18]. This is far more topics than the Encyclopaedia Britannica, with the somewhat contentious claim of comparable accuracy and correctness [4, 9]. Wikipedia has become the modern-day trusted desk reference for almost any topic, yet few users know or care who the specific contributors of the articles are.

Interestingly, the breadth of such social networking resources does not necessarily correspond with a loss of detail. Because the medium of the internet is so pervasive, we can observe that any occurrence can be recorded and immediately disseminated. Many public figures and celebrities have become famous examples of the victims of this kind of information dissemination, with incidents as minor as slips of the tongue or as damaging as alleged racist or sexist remarks. In 2006, Virginia Senator George Allen's controversial remarks during a campaign speech were captured on video, complete with his dismissive voice inflection and mannerisms. The dissemination of that video on *YouTube.com* is widely blamed for his loss in the election that year [14].

Another distinct use for Wikipedia has recently been observed: that of a news medium. Because witnesses and participants have ubiquitous access to Wikipedia as an information repository, they can share their experiences without the need for a reporter or news organization. If the entire user community realizes this potential and takes advantage of this outlet, the composite story of an event unfolds quicker and with more detail there than through any other medium.

The growth in content and influence of net-centric information sources has become a topic of study in itself. They have been modeled as complex dynamic networks and compared to societies of organisms and have been observed to grow at exponential rates. One study also examines the characteristics of the users over the growth cycle [10]. In that study, it is suggested that although the initial users are the "elite" technologically progressive early adopters, it is the "masses" of common users that begin to dominate. In the case of Wikipedia, that happened after only three years, when the number of articles was "only" approximately 100,000. An analysis of the online collaborative information site del.icio.us, which has an entirely different user interaction model, shows a similar behavior [10].

If from these observations we can draw the conclusion that network-centric information environments are quick to attract common users/consumers as the dominant participants, then the effect of this dynamic on military organizations will be of interest, because it clearly has the characteristics of a disruptive technology.

Implications for Military Command and Control

The two side-effects of the move toward net-centric military operations that we consider are *information non-attribution* and *control decentralization*.

Information non-attribution[1] is the effect that follows most directly from the preceding discussion, so it will be discussed first. It is feared in [15] that because net-centricity allows anybody to contribute information in equal formats, such as in the Wikipedia model, the metadata standards will allow all information to be traced back to its provider, increasing the accountability of the source.

Although data standards do indeed support the recording of the pedigree of each piece of information, observations of social networking, blogs, and online collaboration sites show the opposite trend. Many people remember the subject and content of the information, but few bother to check or pay much attention to the provider. We usually either assume that an open public medium provides some measure of quality control, or we grow complacent from the fact that we have received accurate information from there before. We remember Senator Allen's remarks, but not the name of the man who

[1] Whereas the information assurance community often uses the term *attribution* to mean the assignment of *blame*, we use the term here in its broader sense, which is to assign provenance without value judgment on the subject data.

recorded them. We actually do not consider that information important. In the military context, net-centricity is most often proposed for dissemination of situation awareness data. Assuming an acceptable level of communications security that relieves us of the worry of spoofed data, the network will then be used to transmit ISR (intelligence, surveillance, and reconnaissance) data, troop movements, situation reports, etc. In the normal course of a warfighter's workflow, it is unlikely that the source of each such report will be checked.

The infosphere will be considered a trusted pool of information to be used in a distributed and asynchronous way. Likewise, that pool of capability must represent something that can be tasked. In our previous example of the request for a map of New York City, the requester need never know who provided the map to the infosphere or, in fact, if it exists there. If it does not exist in the form desired, an intelligently managed infosphere ought to be able to assemble this information from the pieces that it has available. In terms of the Air Force's Joint Battlespace Infosphere (JBI), this can be done with the aid of a *fuselet* [17]. In commercial technology, this is analogous to a mash-up. In either case, the important feature is that it was the infosphere itself that was tasked, not any specific individual. The individuals no longer matter.

This principal extends to other kinds of requests. Using the principal of effects-based operations (EBO), modern military doctrine includes the concept that it is the '*what*' that is ordered, not the '*how*'. Only the effect is important. If the infosphere includes knowledge of the capabilities of different actors, their current availability status, and their tasking protocol, then like assembling a picture, it can possibly also assemble an action. Therefore, if a commander issues an order for a ground route to be interrupted, EBO doctrine dictates that he should be indifferent to how it is done; be it by dropping any of a number of bombs, from any of a number of platforms, or simply by raising a drawbridge.

So together, we have the phenomenon that net-centric operations lead to situations where ISR might originate from, and command might be issued to, nothing more specific than the *infosphere*. Hence, both information and command lose their attribution; i.e., individuals who are personally responsible. All information exchanges pass through the infosphere, as in Figure 3. Such a concept completely short-circuits the military's traditional hierarchical command structure [11]. As a result, one can imagine higher-order effects in terms of the chain of responsibility (what happens when this process fails?), and the traditional OODA (observe/orient/decide/act) loop. When operations flow through the infosphere, it is difficult to close a loop around specific entities responsible for the four tasks [11, pp. 4 - 5].

This also suggests another change needed for modern C2: somebody to manage the infosphere. If this is now the critical mode of C2, then it is the instrument of dominance, and the outcome of conflicts will be determined by the superiority of the infosphere. This requires a re-consideration of the roles and responsibilities of the warfighter. Distributing information carries with it the burden of managing that information. Users must manage and assure its proper flow, synchronize it, and return observations back to the infosphere from their local vantage point. Alberts refers to this function as the "sensor network manager" [1, p. 83].

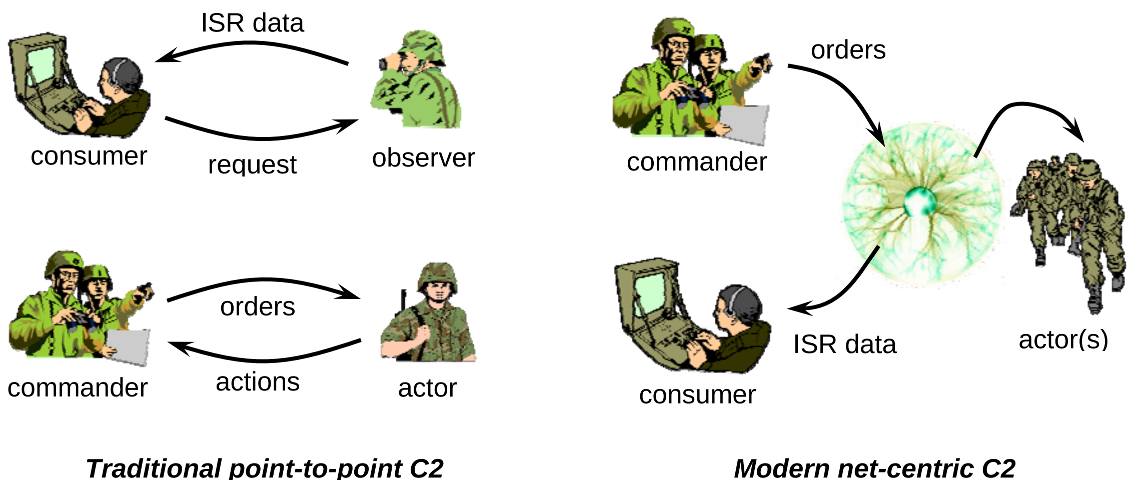


Figure 3. Traditional C2 involves individually indentified sources and sinks. Net-centric C2 allows orders to be issued to "nobody in particular," and information to be received from "nobody in particular."

Case Study: DARPA HURT program

In 2004, the Defense Advanced Research Projects Agency (DARPA) embarked on an effort to provide warfighters on the battlefield with a direct capability to request and receive combined ISR data and common operational pictures (COPs). Traditionally, such requests were relayed to operating centers where the specific request was received and matched with data available. If the data was not available, higher authority would have to be granted in order to task an ISR asset to collect it, then the operations center would have to manually route it to the requester, a process that could take an indeterminate amount of time.

Under the Heterogeneous Urban Reconnaissance Team (HURT) program, the warfighter would instead simply ask the system for imagery of arbitrary objects or areas, or even ask for persistent sensing, such as for force protection or surveillance. He would not specify an asset or other specific source for this information, just the *content* he needed [3].

To fulfill the request, the system would either match it with a data store, or determine that the information did not exist. If this is the case, the system invokes an asset allocation and planning process that would collectively task and synchronize one or more assets to gather the needed information. It then supervises and controls the gathering operation, fuses it as necessary, and manages the transfer of that information back to the user.

This is an example of a military system that recognizes the possibility that tasks need not be issued to specific battlespace entities, and information need not be sourced from a specific sensor or database. It is a true example of net-centric ISR operations, as illustrated in Figure 4.

However, in the early days of the program, there was resistance among the military to adopt the concepts of shared control. Traditional ISR assets are “owned” by somebody who has direct control of them and their data. Early users were skeptical that it would be to their benefit to relinquish sole control of their assets, and they feared that sharing information would dilute their access to the asset. To a small extent this was true, but eventually it became clear that it is not the *asset* that it valuable to them, but the *information* that was available to them. By working through the shared information space, their locally-produced ISR data would be combined with data provided by other team members and result in a much richer data set that would be equally available to them and their warfighting partners, making them more effective as a team. It was a change in culture to work directly with *information* as the commodity of their work.

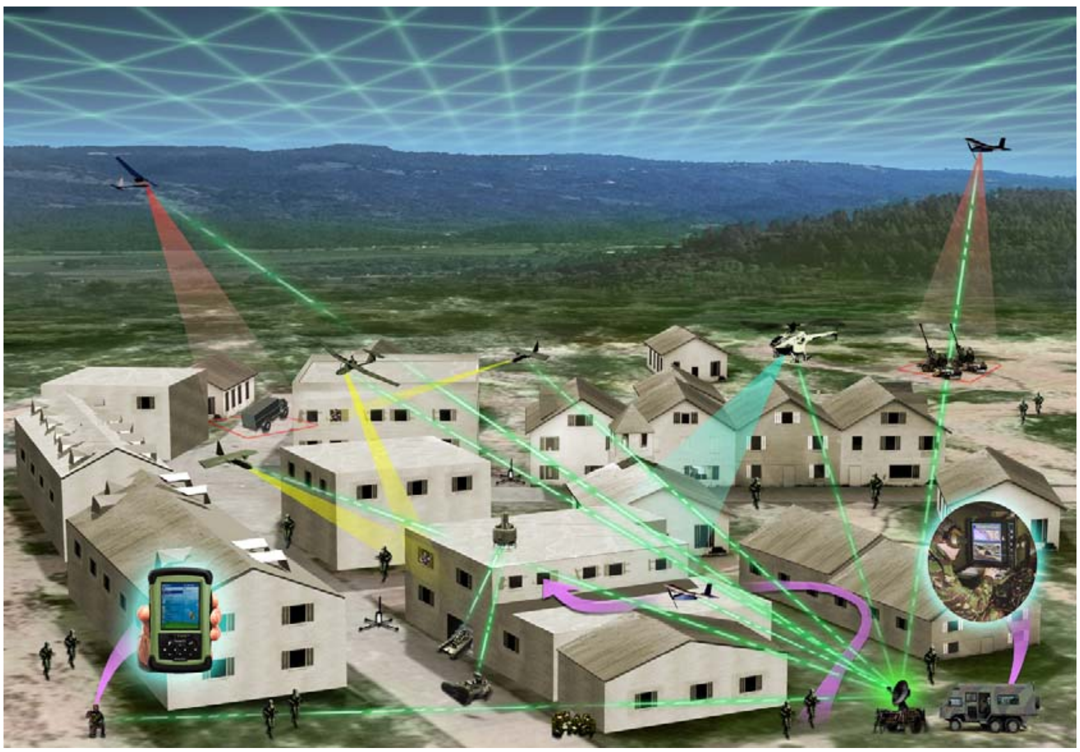


Figure 4: The HURT concept allows warfighters to request imagery and operating pictures without tasking individuals or assets. If the requested information is not available, the system automatically tasks available assets and fulfills the request.

A similar observation may be made in the case of fighter aircraft. In the early concepts and design of the F-22A, that aircraft’s impressive ISR capabilities were kept on-board, to serve only the situation awareness needs of the pilot. Being a stealth aircraft, the intent was to keep the platform from emanating radiation that would betray its presence. Indeed, the aircraft has no digital downlink; its digital information is receive-only. However, as the utility of this ISR data was found to grow both horizontally (in the types of consumers who needed it) and vertically (in the command hierarchy; i.e., using the data at operational and tactical levels), there was more pressure to distribute this data to receivers on the ground.

Control Decentralization

Military command has historically been based on knowledge. Commanders have been located in operations centers in order to create a central node for the knowledge necessary to wage the battle. This knowledge was in a tangible form, such as in maps or transcribed communications that made a centralized location a practical necessity. The command center was the only place where sufficient knowledge was gathered to effectively manage a battle or campaign. The size of the fighting units was tied to the span of command, control, and communication (C3) of the commander. The larger the scope of control, the larger, and usually more remote, the command center would be. In many campaigns since World War II, planning and command was performed on a different continent from the actual conflict. Even in those historical cases, this practice proved ineffective because of the latency and lack of local situation awareness that resulted [11].

However, the second major influence of the widespread adoption of net-centric operations is the concept of control decentralization. In control decentralization, the initiative, decision-making, and responsibility for tactical actions is bottoms-up. The warfighter has direct access to theater-wide situation awareness data, and is fully aware of his own role and his unit's context in the fight. He is able to directly communicate with weapons platforms and can assess effects. The knowledge needed to fight the war is not consolidated in the command center but is equally available to all. The concept of "command" is not enabled by the consolidation of information and the span of control around the command center or commander, it is distributed. As observed in [15], control decentralization has already been anecdotally observed, while in fact observations supporting the migration of control to tactical edges have a much longer history [11].

The conclusion in [15] is that the presence of an infosphere tempts the commander to micro-manage by giving him the impression that he has all the information necessary to direct the battle. Indeed, Czerwinski refers to this form of command as *command-by-direction*, and suggests that this tendency exemplified by the Army's "Force XXI" digitized battlefield concept. The drawback, though, is that uncertainty (pervasive on the distributed battlefield) is poorly managed by such centralized authority. Even though bits may travel at the speed of light, change that occurs on the battlefield propagate with measureable latency, and data synchronization and reconciliation take significant amounts of time to resolve.

In contrast, Czerwinski's *command-by-plan* is more representative of the Air Force's C2 tenet "Centralized Control, Decentralized Execution" [2, 8]. This form of command is largely strategic and is dominated by centralized planning, therefore tending to also centralize uncertainty and focus on an opponent's centers of power. Operating in this mode actually reduces the force's reliance on real-time information and therefore reveals its weaknesses when directed at adversary's without persistent centers of power (such as in the global war on terror).

The alternative to these types of command is *command-by-influence*. According to Czerwinski, this mode of command is most consistent with the empowerment of forces in the field to take locally-controlled initiative, guided by the commander's intent. Overall control is an emergent property of a force that is complex in structure and relationships, but loosely-coupled by control, by virtue of more decentralized execution authority. Only in this way can uncertainty be adequately managed, and this may be the reason that command is observed to be reverting to the actors; being decentralized to an unprecedented degree.

As decision-making becomes more localized, it can be observed that the control and execution functions become indistinguishable. This will be more apparent in the information domain than in any other.

Control and Execution in Cyberspace

In 2005 the Air Force declared *cyberspace* to be a warfighting domain, peer to *air* and *space*. In some ways it is easy to think of cyberspace as a domain. Conflicts occur there, transactions take place, partnerships form, and assets are lost and gained. However, in many ways it is quite different from air and space. Cyberspace has no physical dimension. All principals of command and control that trace their roots back to physical span of control and battlefield dimensions must be reconsidered. Indeed, some of cyberspace's most intimidating aspects as a domain of conflict are its low cost of entry and its total lack of physical boundaries. So if we consider this domain against the Air Force doctrine of "centralized control, decentralized execution," then we must ask, "central to *what*?" If this question has no answer, then perhaps we need to re-evaluate the doctrine.

Because the assemblage of information in the infosphere implies no spatial proximity, and the field of battle itself has no relevant physical dimension, warfighting in cyberspace might be considered the limiting case of net-centric warfare. As [1, p. 62] points out, network-centric operations have little effect on the cost of moving people and materiel (a claim that might be arguable to the network-centric logistics community), so its influence on warfighting is to do more while leaving materiel "things" where they are. Taking this to its logical conclusion, warring parties who rely more and more on their information dominance will fight battles with fewer and fewer physical entities: the cyber-war.

The cyberspace domain, then, illustrates the merging of C2 and execution functions: the ultimate control decentralization.

Conclusions

What we have attempted to do here is to ascribe a causal relationship between observed C2 trends and behaviors and the properties of net-centricity as a disruptive innovation. In this regard, the sudden "loss" of performance at the time of disruption was identified as a loss of information attribution and the decentralization of control. In the manner of disruptive innovations, though, this loss of performance is due to changing value sets associated with the technology, so that as the disruptive technology becomes more familiar, its attributes are more fully appreciated, and the performance of the technology is expected to surpass that of a sustaining technology.

Perhaps a more useful endeavor is to predict additional effects of net-centricity on command and control. First, as these behaviors are recognized, the role of the commander is important. In order for decentralized control to function effectively, the role of commander's intent is more critical than is commander's direction. In a net-centric environment, this means more than simply the formal expression of operational orders, but rather, that the implementation of this intent must move toward being a continuous adaptive process, yet one that does not subsume the competencies of actors. It will need to move to a machine-readable form, and with automated weapons perhaps evolve into a machine-to-machine message. In his new role, the commander will also function as an information router, or more appropriately, an information *manager*, recognizing where information is lacking or incorrect and serving new information to the distributed actors.

The implications of disruptive innovation in the military were recognized in [13], where it was suggested that military leaders bear the responsibility to "disguise" innovation. By this, Pierce means that truly disruptive innovations are more readily accepted if the disruptions are disguised as sustaining innovations. That is, that the new values of the technology should be treated as the natural progression of the old values. In this situation, the implication is that commanders should begin to empower their tactical units to act with local initiative on commander's intent even before true net-centricity is widely available.

As a result of disguising the innovation and the consequence that execution and decision-making merge and are increasingly performed at tactical edges, the commander will also need to act as the *authorization agent*. As suggested in [11], the lower levels of the military hierarchy are naturally growing more capable by virtue of the information they possess, but they may be "paralyzed by political limitations and will not have any initiative" [11, p. 5]. In order for this not to happen, the commander will have to take an active role in securing and verifying authority for the actions taken by his remote forces. Battle management may take more of a command-by-consent character.

As observed by Czerwinski [6], net-centric systems evolve into a loosely-coupled yet complex dynamic system, and are therefore apt to generate emergent dynamics or chaotic behaviors. If this is true, then it is the commander that must exert the stabilizing supervisory influence, but not through literal direction. The appropriate emphasis is on new types of training, so that the distributed forces maintain their initiative to execute opportunistically, but within the structure of the newly-fortified form of commander's intent. Thus, the behavior of the commander will be less like a *director* and more like a *conductor*.

Finally, it must be realized that the adoption of new technologies is never done by unanimous consent. There will be resistance and resistive behaviors that should be predicted and controlled. One of these would be the temptation to restrict information flow to those who could make use of it merely to preserve a command hierarchy that demands a segregation of information. Aside from being technologically counterproductive, such a strategy inevitably ends in failure.

References

[1] Alberts, David S. et al, *Network-Centric Warfare: Developing and Leveraging Information Superiority*, CCRP Publication Series, 1999.

[2] *Air Force Basic Doctrine*, Air Force Doctrine Document 1, http://www.dtic.mil/doctrine/jel/service_pubs/afdd1.pdf, November 2003.

[3] Bay, John S., “Demonstrating Tactical Information Services from Coordinated UAV Operations”, *SPIE Conference on Defense Transformation and Network-Centric Systems, Defense and Security Symposium*, April 2006.

[4] Berinstein, Paula, “Wikipedia and Britannica: The Kid’s All Right (And So’s the Old Man)”, *Information Today*, vol. 14, no 3, March 2006.

[5] Christensen, Clayton M., *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, Harvard Business School Press, 1997.

[6] Czerwinski, Thomas, J., “Command and Control at the Crossroads,” *Parameters*, Autumn 1996, pp 121 – 132.

[7] Department of Defense, *Net-Centric Environment Joint Functional Concept*, version 1.0, April 2005.

[8] *Doctrine for the Armed Forces of the United States*, Joint Publication 1, http://www.dtic.mil/doctrine/jel/new_pubs/jp1.pdf, May 2007.

[9] Giles, Jim, “Internet Encyclopaedias Go Head to Head,” *Nature*, vol. 438/15, December 2005.

[10] Kittur, Aniket, et al., “Power of the Few vs. Wisdom of the Crowd: Wikipedia and the Rise of the Bourgeoisie,” *Proceedings of Computer/Human Interaction conference*, 2007.

[11] Kometer, Michael W., *Command in Air War: Centralized Versus Decentralized Control of Combat Airpower*, Air University Press, 2007.

[12] Network Centric Operations Industry Consortium, *https://www.ncoic.org/wiki/NetworkCentric*, 2007.

[13] Pierce, Terry C., *Warfighting and Disruptive Technologies: Disguising Innovation*, Frank Cass Publishers, 2004.

[14] Rich, Frank, “2006: The Year of the ‘Macaca’”, *New York Times*, November 12, 2006.

[15] Rosenberg, Barry, “Common Knowledge: Can leaders stay effective when troops have access to the same information?” *C4ISR Journal*, vol. 6, no. 8, September 2007.

[16] Stenbit, John P., *DoD Net-Centric Data Strategy*, 2003.

[17] USAF Scientific Advisory Board Report on *Building the Joint Battlespace Infosphere, Volume 1: Summary*, SAB-TR-99-02, 17 December 1999.

[18] Wikipedia Statistics, http://en.wikipedia.org/wiki/Special:Statistics.

Disruptive Effects of Net-Centricity on Command and Control

Dr. John S. Bay, ST

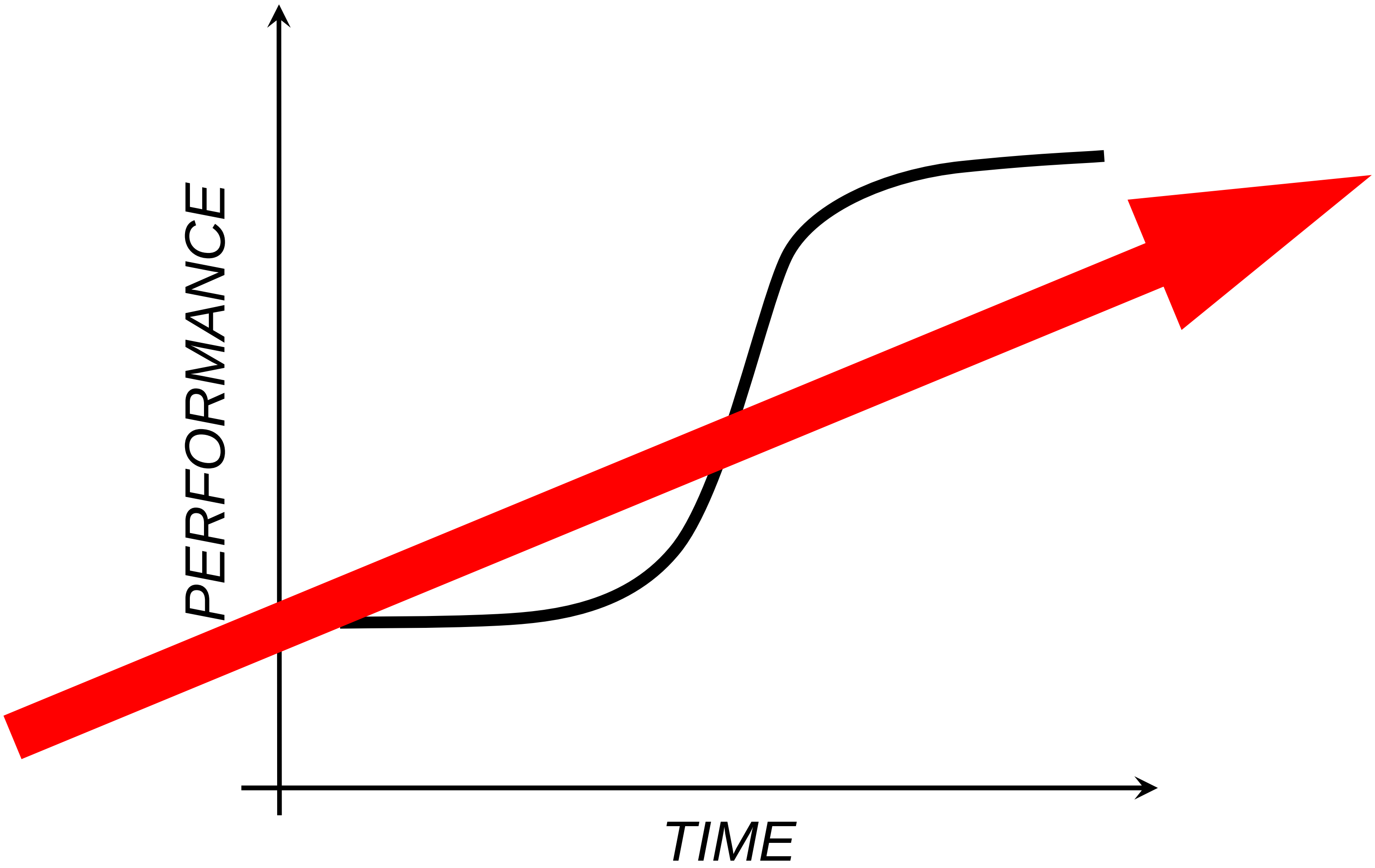
Chief Scientist,

Air Force Research Laboratory, Information Directorate

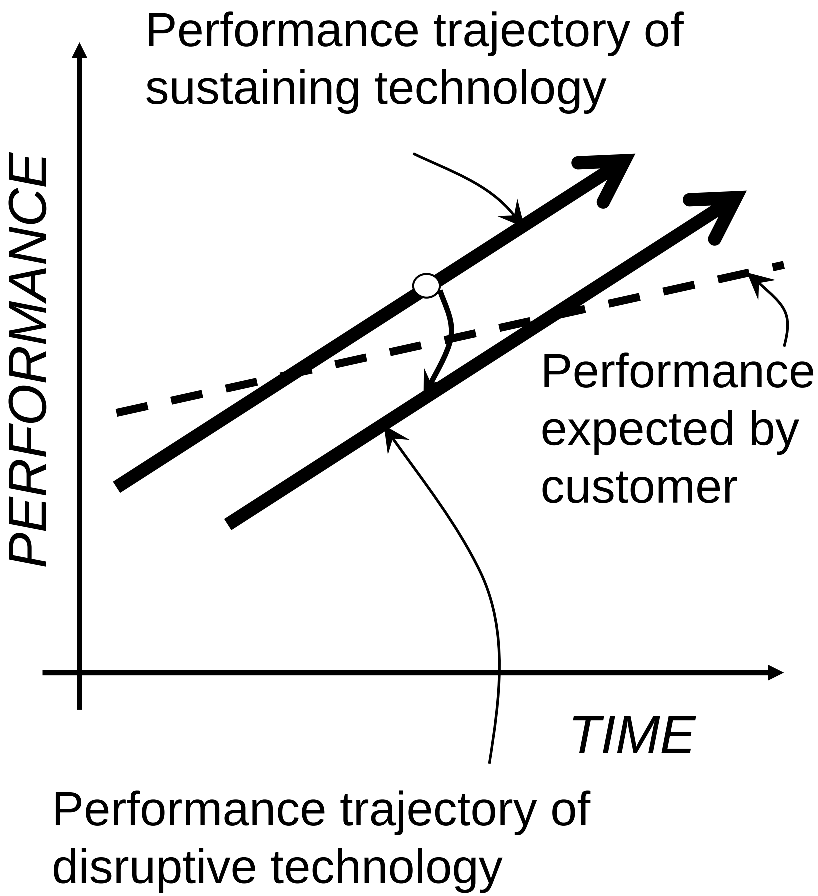
Overview

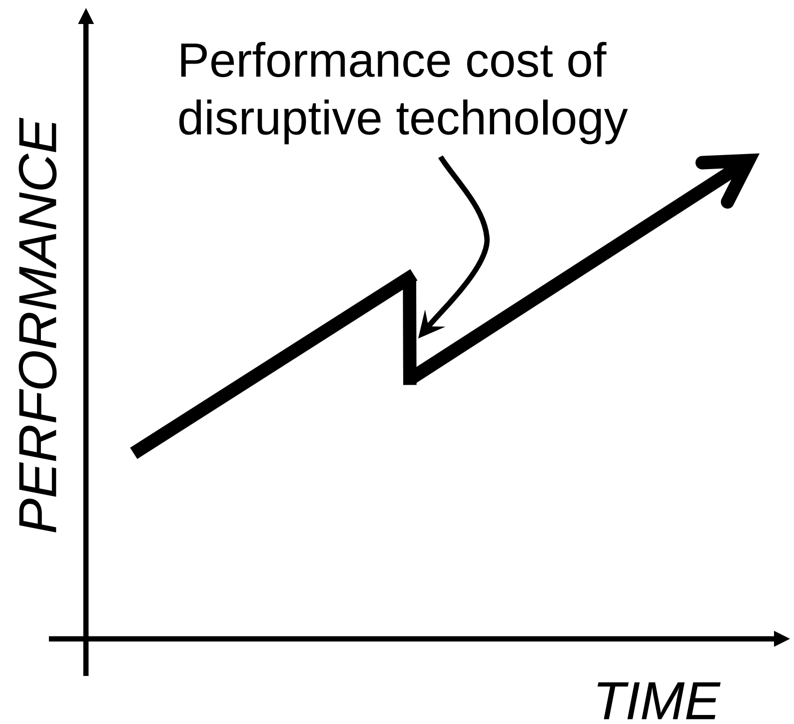
- Philosophical view of net-centricity
- It’s here! Power to the people!
- Wait! That’s not how we do things …
- Innovation at a cost
- The good news and the bad news
- Predicting and preparing for the future

Disruptive Innovation



Disruptive Innovation





Net performance as majority of customers defect to disruptive technology

Information Explosion

- World War I: 30 Words per Minute
- WW II: 60 Words per minute
- Vietnam: 100 Words per minute

Gulf War: 192,000 Words per minute

War in 2010: 1.5 trillion Words per minute

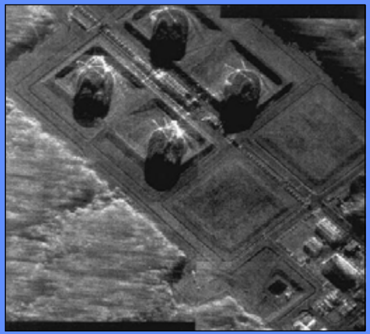
U.S. News & World Report

Managed Information

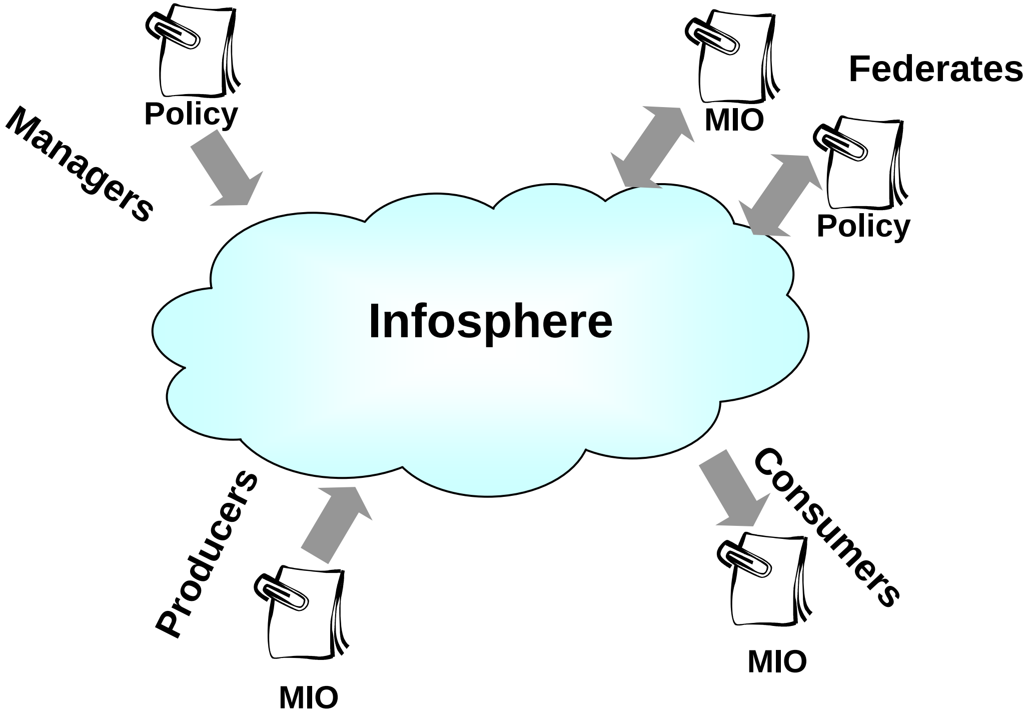
Infosphere Information Exchange Unit

Managed Information Object (MIO)

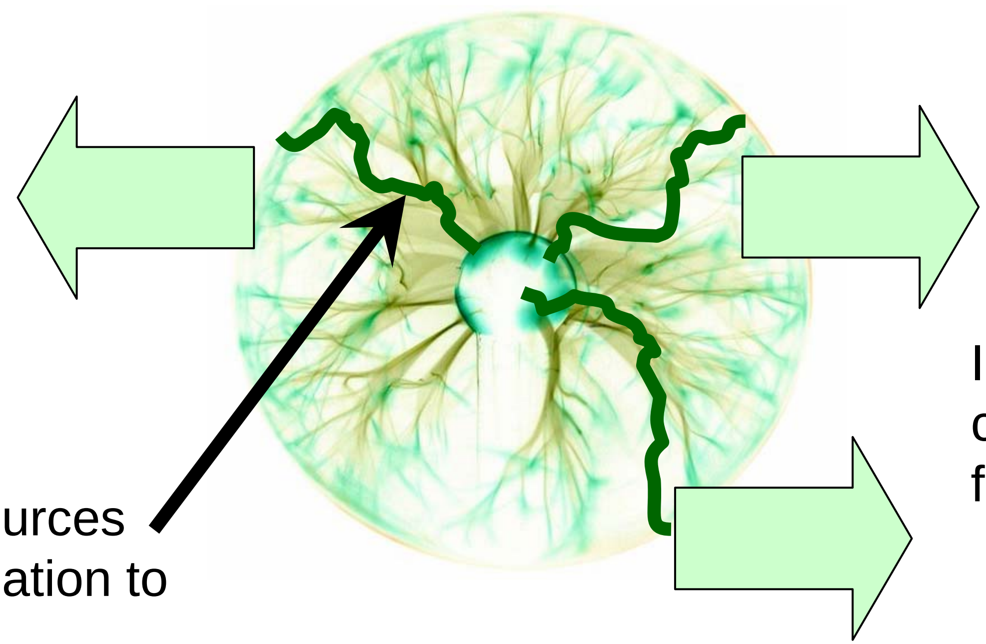
<metadata>
<baseObject>
<InfoObjectType>
<Name>Image</Name>
</InfoObjectType>
<Publisher>Intel COI
</Publisher>
<Latitude>28.2.3
</Latitude>
<Longitude>54.3.46
</Longitude>
</baseObject>
</metadata>



Establishment of Shared Information Space



Net-centricity

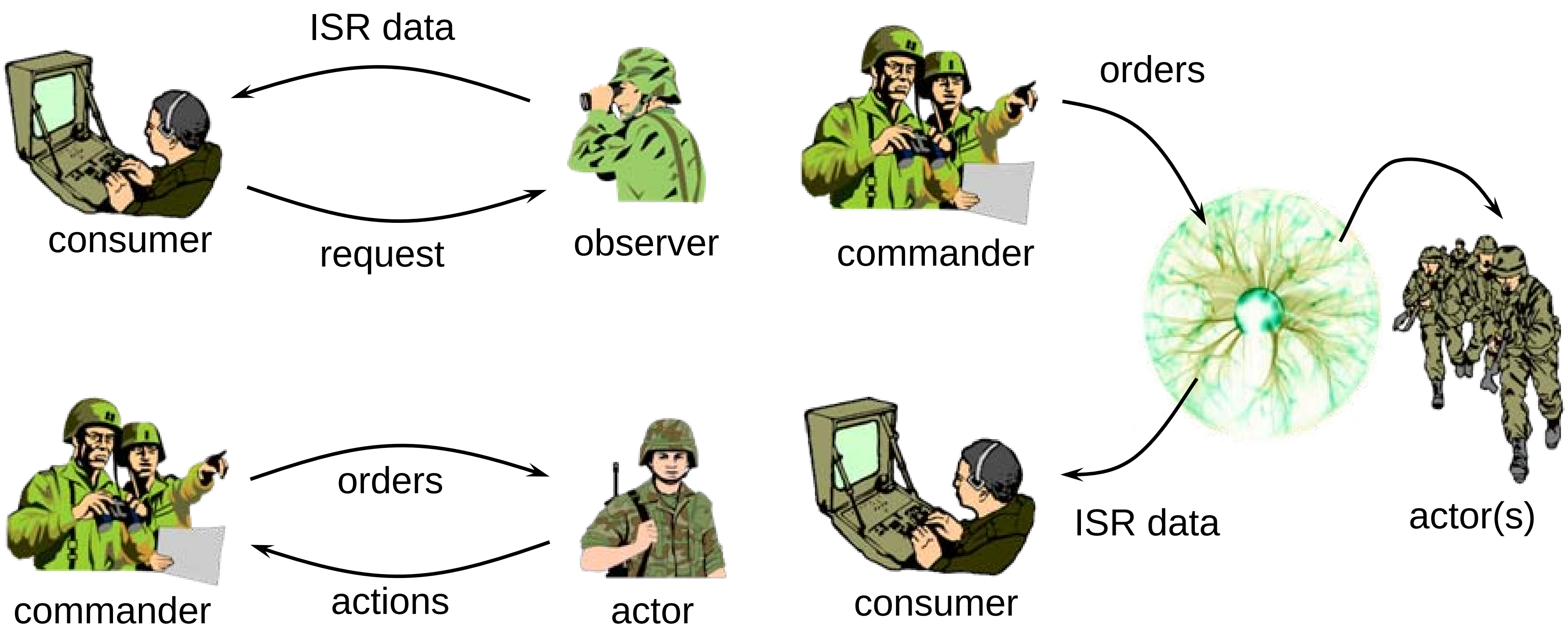


Information sources provide information to the sphere

Information consumers draw from the sphere

Net-Centricity, The Movie

Implications



Traditional point-to-point C2

Modern net-centric C2

Information Non-Attribution

HURT Program

Command Modes

- **Command-by-direction**
  - **Centralizes uncertainty**
- **Command-by-plan**
  - **Prioritizes uncertainty**
- **Command-by-influence**
  - **Distributes uncertainty**

Centralized vs Decentralized Control?

- Does this dynamic encourage micromanagement or decentralized control?
- Consider other social networking capabilities/phenomenon

Control Decentralization

- **Contrast to command-by-direction**
- **Fully supports *commander's intent***
- **Compare to *loosely-coupled complex dynamic system***
- **Ultimate realization: *C2 in cyberspace***
  - **No physical AORs**
  - **Actors are remote**
  - **Threats are distributed**
  - **A driver of *policy-based decision-making***

The Future

- **Increasing role for *commander's intent***
  - **Formal M2M expressions**
  - **Role as the *information manager***
  - **Authorization agent**
- **Disguising Innovation**
- **Less *direction*, more *orchestration***
- **Cyber warfare**
- ***The gatekeepers of information***

Questions/Discussion